

## Podporované OS

- Microsoft Windows 2000, 2003,
  - XP a Vista
- Apple Mac OS 10.4.6 (Tiger)

## Šifrovací API

- PKCS #11 v2.01
- Microsoft CryptoAPI (CAPI) 2.0
  - Microsoft PC/SC
  - Apple Native PC/SC

## Délka šifrovacích klíčů

- RSA 512 až 2048 bit

## Šifrovací funkce & Algoritmy

### Asymetrické klíče

- RSA

### Symetrické klíče

- DES, 3DES

### Elektronický podpis

- RSA, DSA

### Hashovací funkce

- SHA-1

### Výměna klíčů

- RSA
- Diffie-Hellman
- Vytváření klíčů na kartě
- DES hardwarový koprocessor pro bezpečné vytváření klíčů na kartě

## Paměť EEPROM

- Kapacita 32K

## Odpovídá

- FIPS 140-1/2 úroveň 2
  - ISO 7816
  - GSC-IS v2.1

# Čipová karta model 330

Model 330 čipová karta je smart karta s integrovaným mikroprocesorem, který obsahuje SafeNet SCCOS operační systém (SafeNet Cryptographic Card Operating System).

Karta je podporována klientským softwarem BSec PK nebo BSec SSO (více informací o tomto SW naleznete v sekci Software) a sériovou, USB, PCMCIA, nebo jinou povolenou PC/SC čtečkou čipových karet.



## Vlastnosti:

- Čipová karta dle standardu ISO-7816.
- Schváleno pro FIPS 140-2 úroveň 2.
- Šifrovací koprocessor pro urychlení.
- SCCOS operační systém čipové karty 32K je uložen v paměti ROM.
- 32K EEPROM pro bezpečné uložení klíčů, hesel, certifikátů a dat.
- DES hardwarový koprocessor umožňující šifrování tajných klíčů přímo na kartě.
- Hardware a software má ochranu proti různým útokům.
- Funkce veřejného klíče (public key):
  - ◇ Generování DSA klíče (klíče o délce 1024-bitů).
  - ◇ Generování RSA klíče (klíče o délce 1024-bitů a 2048-bitů).
  - ◇ RSA/DSA klíče pro elektronický podpis.
  - ◇ Možnost výměny RSA klíčů.
  - ◇ Možnost výměny Diffie-Hellman klíče.
  - ◇ SHA-1.
  - ◇ Možnost šifrovat/dešifrovat pomocí unikátního klíče DES/3DES.

Standardy	ISO-7816- 2, 3, 4; PKCS #1; PKCS #11
Napájení	Maximálně 10mA
EEPROM	32K, neomezené čtecí cykly; zápis/mazání 100 000
Provozní teplota	-25°C to 70°C
Podporované čtečky	Sériové, USB, PCMCIA, Express Card a všechny čtečky podporující PS/SC protokoly
Operační systémy	Windows 95, 98, NT, 2000, XP, Vista

